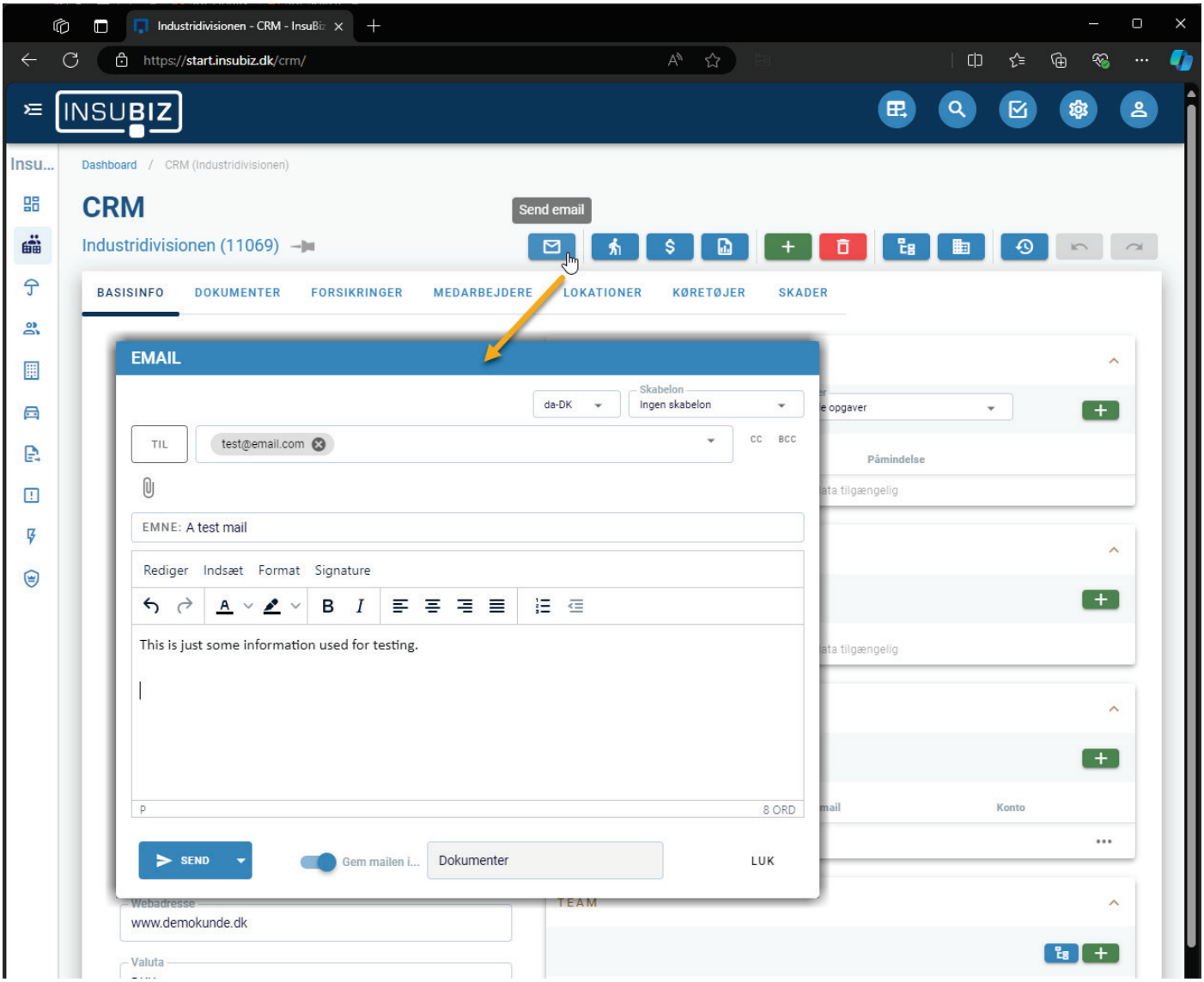
Contents

App description

The InsuBiz Cloud – MS 365 integration (*IB MS365 App*) is used to enable users to send e-mails directly from the InsuBiz Cloud platform using their own MS 365 mailbox or any shared mailbox they have permission to use.

E-mails sent this way, will be journalized in the InsuBiz Cloud solution and will be present in the users Outlook "Sent Items".



Authentication

The *IB MS365 App* uses Microsoft Authentication Library (MSAL) to authenticate users and access Microsoft Graph API.

More information about MSAL can be found here

Security and permissions

The *IB MS365 App* is tenant and user aware.

All permissions required for the *IB MS365 App* are delegated permissions, meaning that the application needs an authorized user login to perform actions on behalf on this user and only the specific user that has been authorized.

The *IB MS365 App* cannot perform actions on behalf of the tenant.

Required permissions

Microsoft Graph			
User.Read	Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Used by InsuBiz Cloud to read basic information used for e-mail purposes.
Mail.Send	Send mail as a user	Allows the app to send mail as users in the organization.	Used by InsuBiz Cloud to send e-mails from the specific user's mailbox.
Mail.Send.Shared	Send mail on behalf of others	Allows the app to send mail as the signed-in user, including sending on-behalf of others	Used by InsuBiz Cloud to send e-mails from shared mailboxes that the specific user has access to.
openid	Sign users in	Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.	Used by InsuBiz Cloud to identify the specific user, and to ensure that the user is authorized. *(Standard in MSAL)**
profile	View users' basic profile	Allows the app to see your users' basic profile (e.g., name, picture, user name, email address)	Used in the sign-in process to read needed user profile information *(Standard in MSAL) **
offline_access	Maintain access to data you have given it access to	Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.	Used by InsuBiz Cloud to be able to request refresh tokens from AAD *(Standard in MSAL) **

** These permissions are required by MSAL*

Permission details

Sign in and read user profile

Resource application
Microsoft Graph

Claim value
User.Read

Permission display name
Sign in and read user profile

Permission description
Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Send mail as a user

Resource application
Microsoft Graph

Claim value
Mail.Send

Permission display name
Send mail as a user

Permission description
Allows the app to send mail as users in the organization.

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Send mail on behalf of others

Resource application
Microsoft Graph

Claim value
Mail.Send.Shared

Permission display name
Send mail on behalf of others

Permission description
Allows the app to send mail as the signed-in user, including sending on-behalf of others.

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Sign users in

Resource application
Microsoft Graph

Claim value
openid

Permission display name
Sign users in

Permission description
Allows users to sign in to the app with their work or school accounts and allows the app to see basic user profile information.

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

View users' basic profile

Resource application
Microsoft Graph

Claim value
profile

Permission display name
View users' basic profile

Permission description
Allows the app to see your users' basic profile (e.g., name, picture, user name, email address)

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Maintain access to data you have given it access to

Resource application
Microsoft Graph

Claim value
offline_access

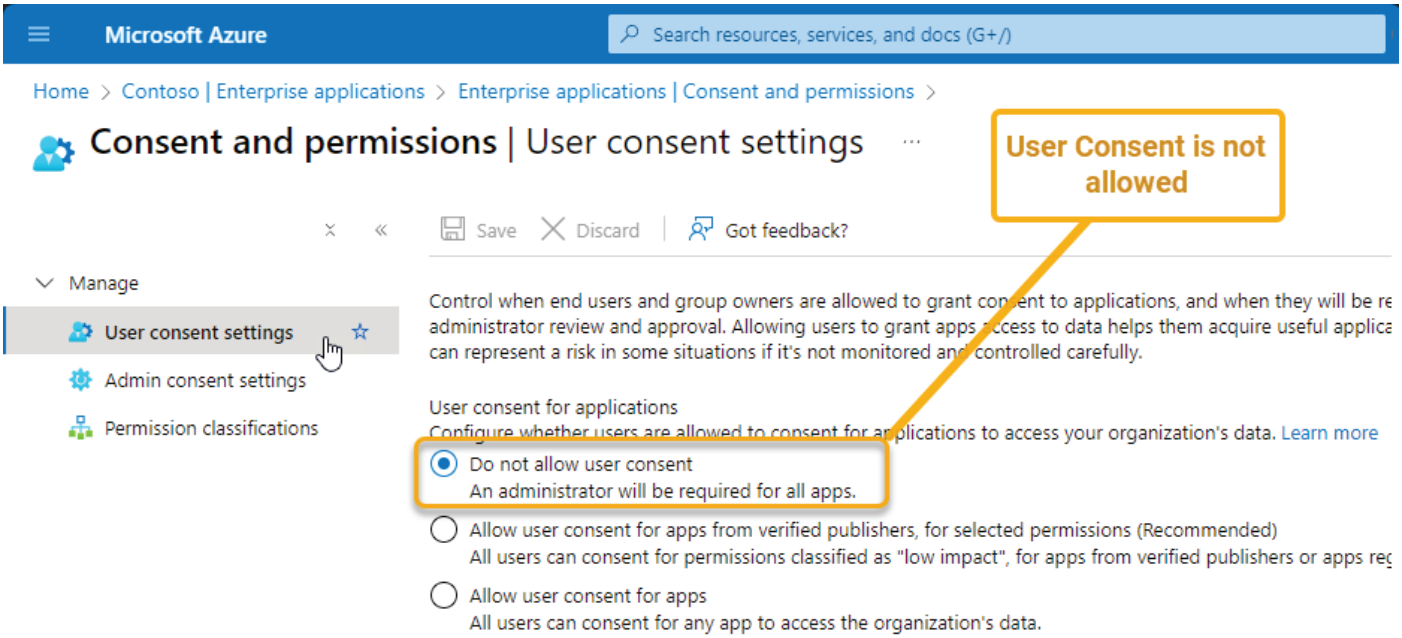
Permission display name
Maintain access to data you have given it access to

Permission description
Allows the app to see and update the data you gave it access to, even when users are not currently using the app. This does not give the app any additional permissions.

Permission type
Delegated. Delegated type means that this application may act on behalf of a user as the user him or herself for this particular permission.

Permission approval and admin consent

It is assumed, that the organization does not allow user consent to applications. Therefor an admin consent will be necessary to allow the users to access the InsuBiz Cloud – MS 365 integration.



Entra Id – Enterprise Applications

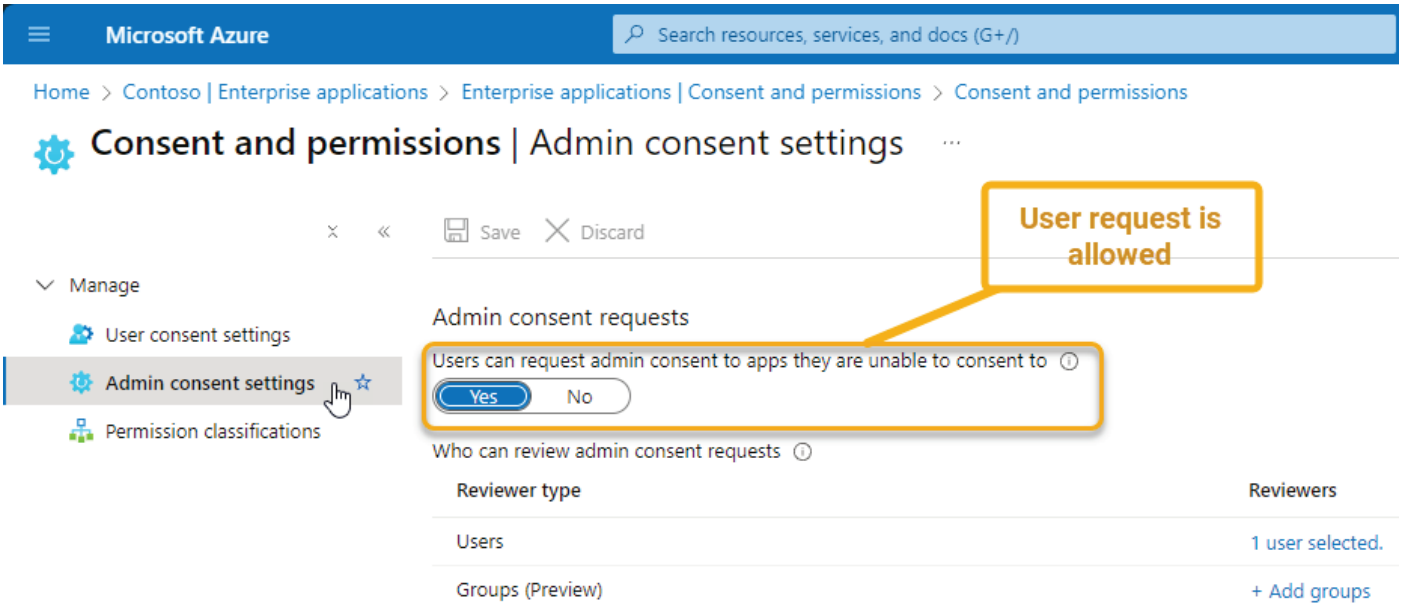
There are two primary methods for setting up the admin consent:

- Admin consent after user request.
- Admin consent using MS identity platform URL.

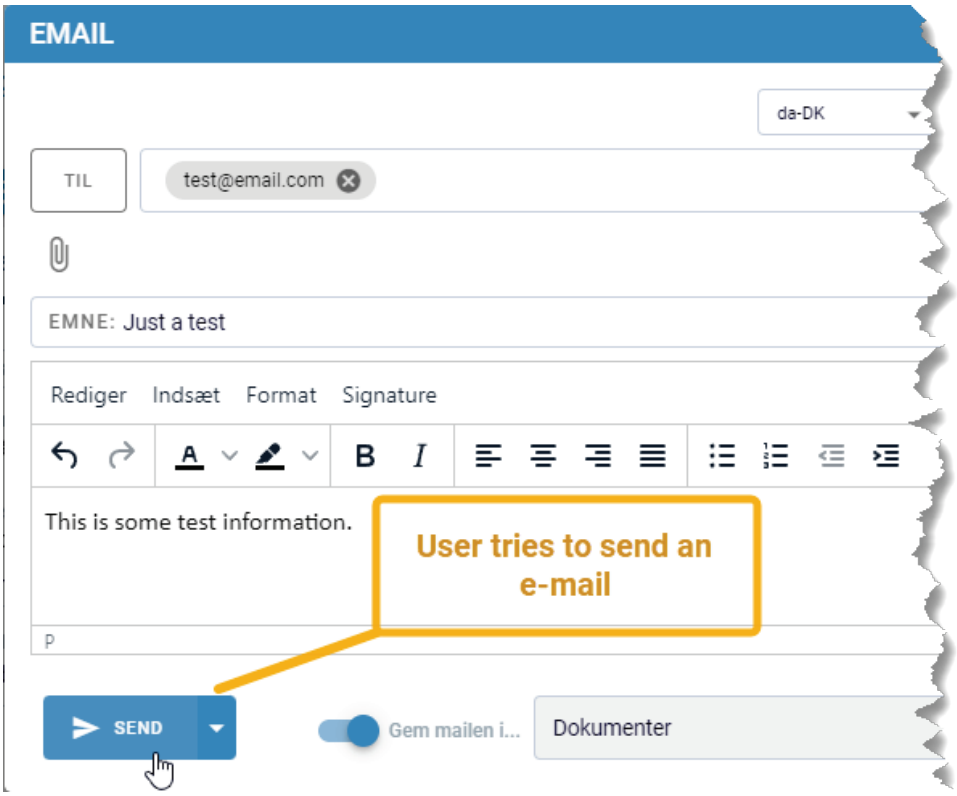
Both will be covered in the following.

Admin consent after user request

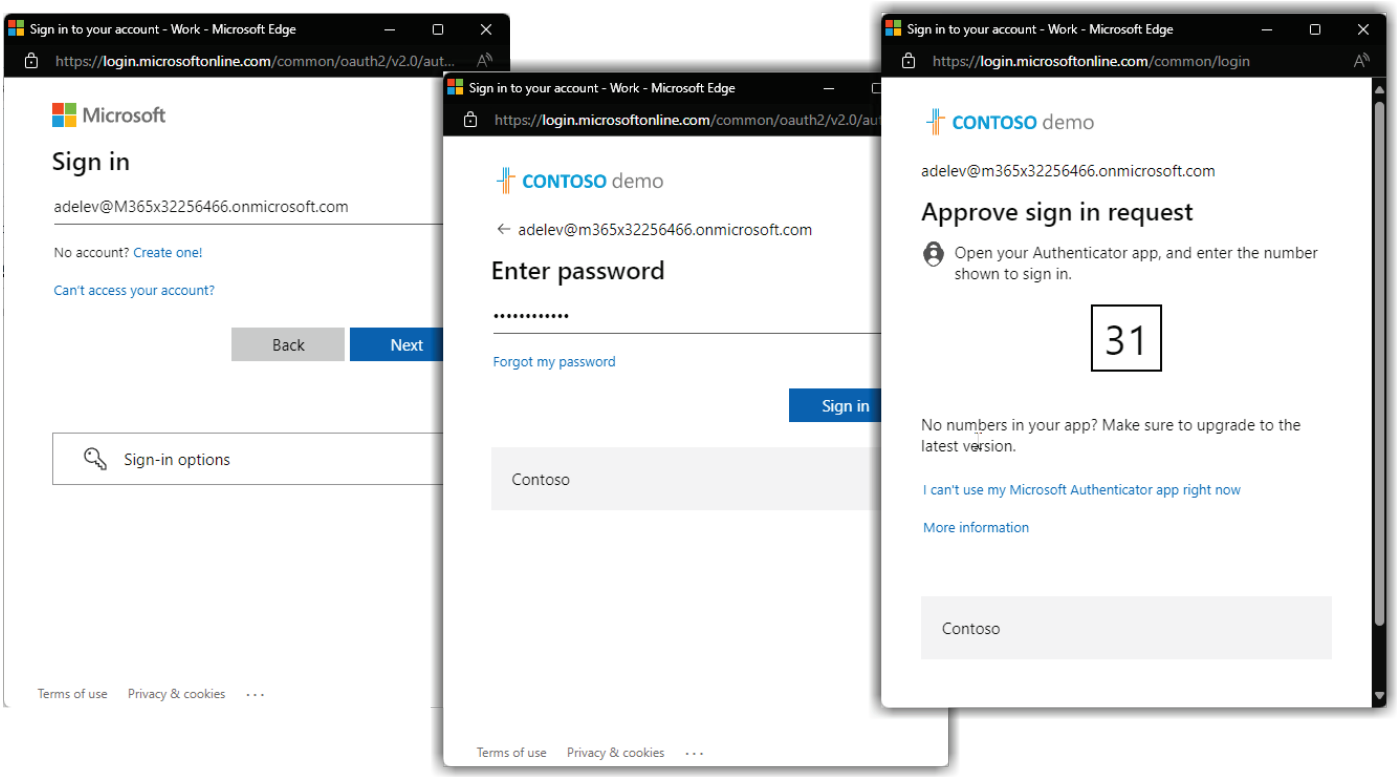
When a user tries to use the e-mail integration functionality in InsuBiz Cloud, the system checks for the required permissions. If the permissions are not granted and users are allowed to request Admin Consent in the organization *(see illustration below),* the user can make a request for admin consent.



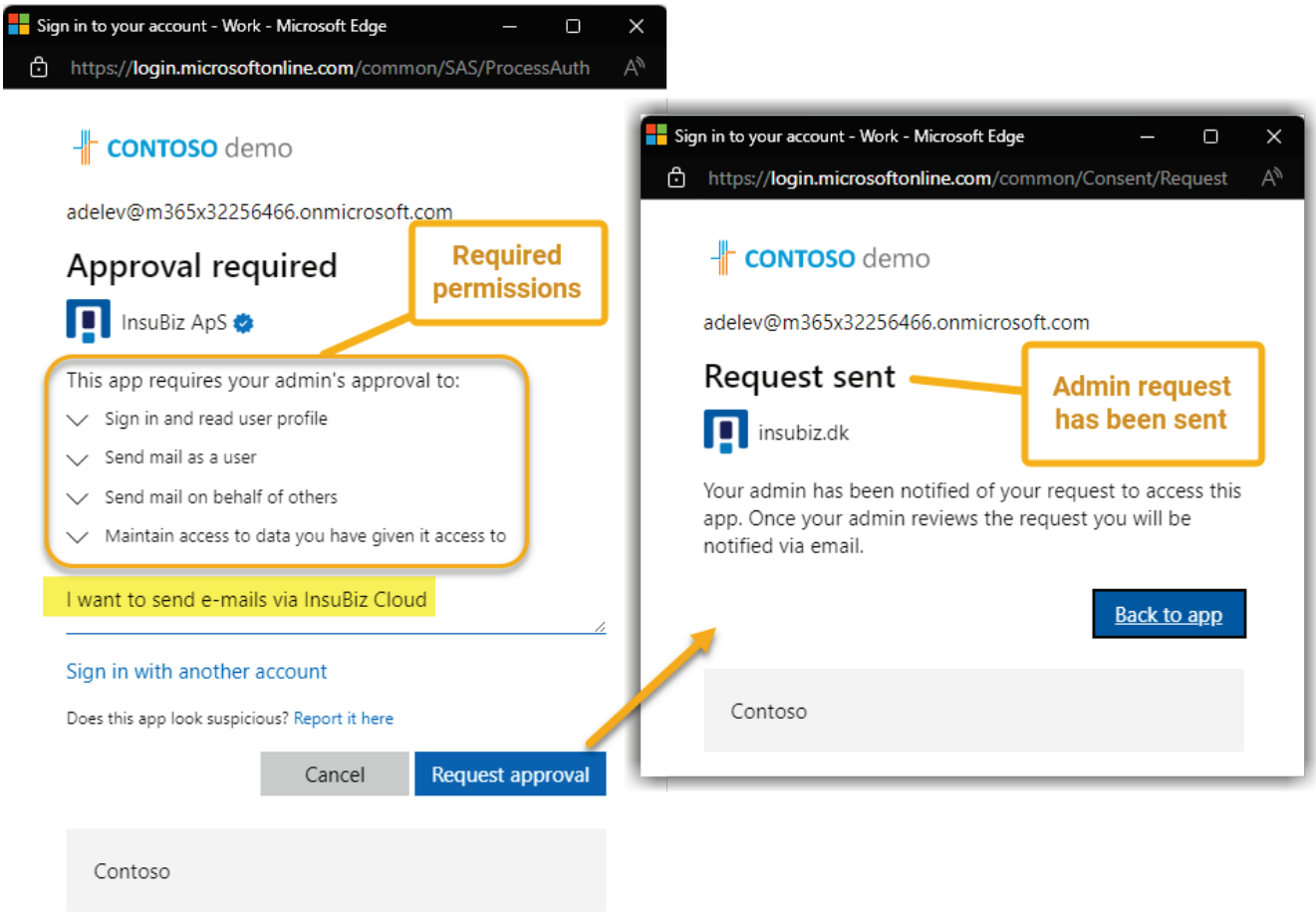
1 User tries to send an e-mail from the InsuBiz Cloud platform



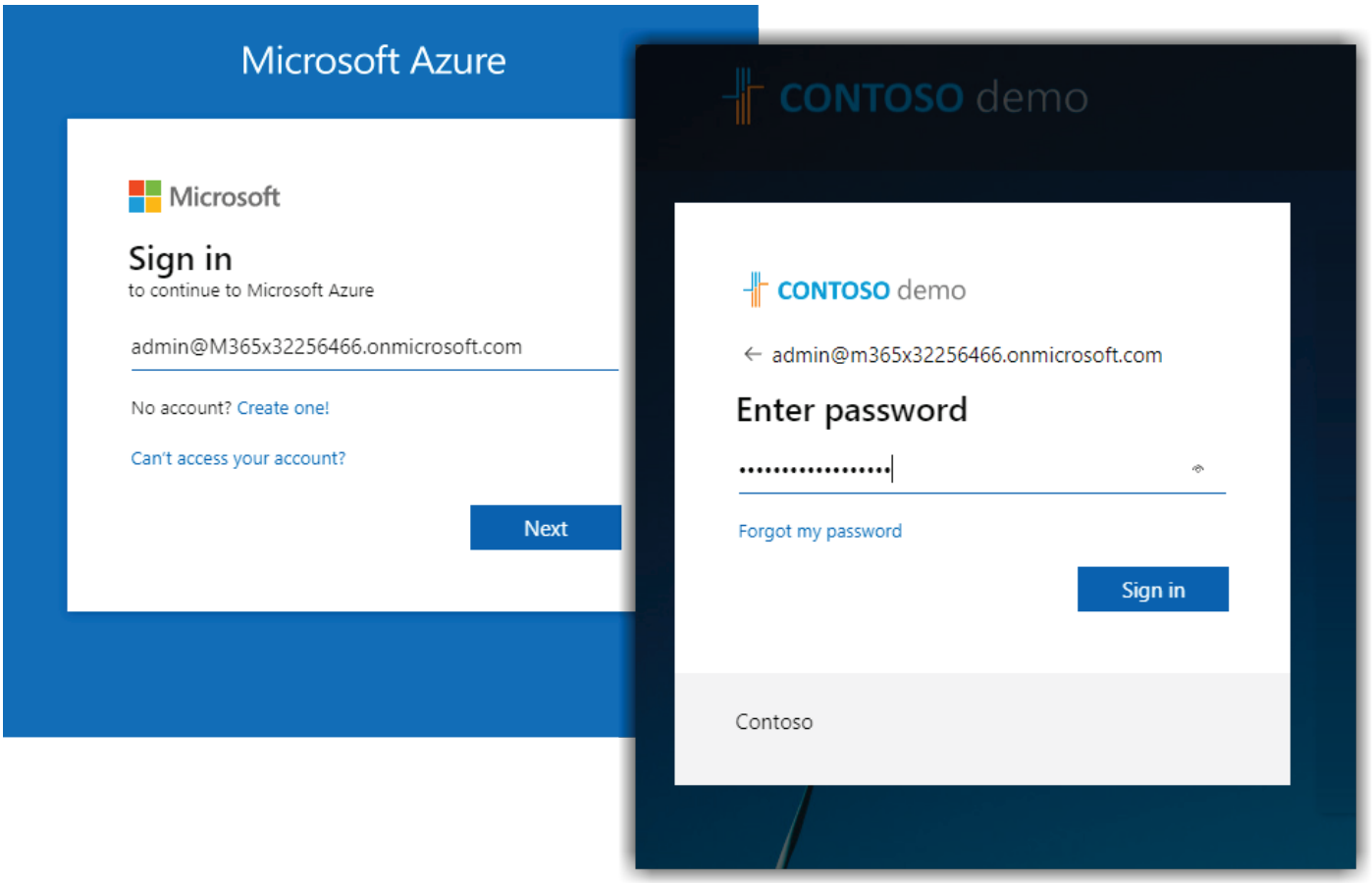
2 User is asked to sign in to their MS 365 account



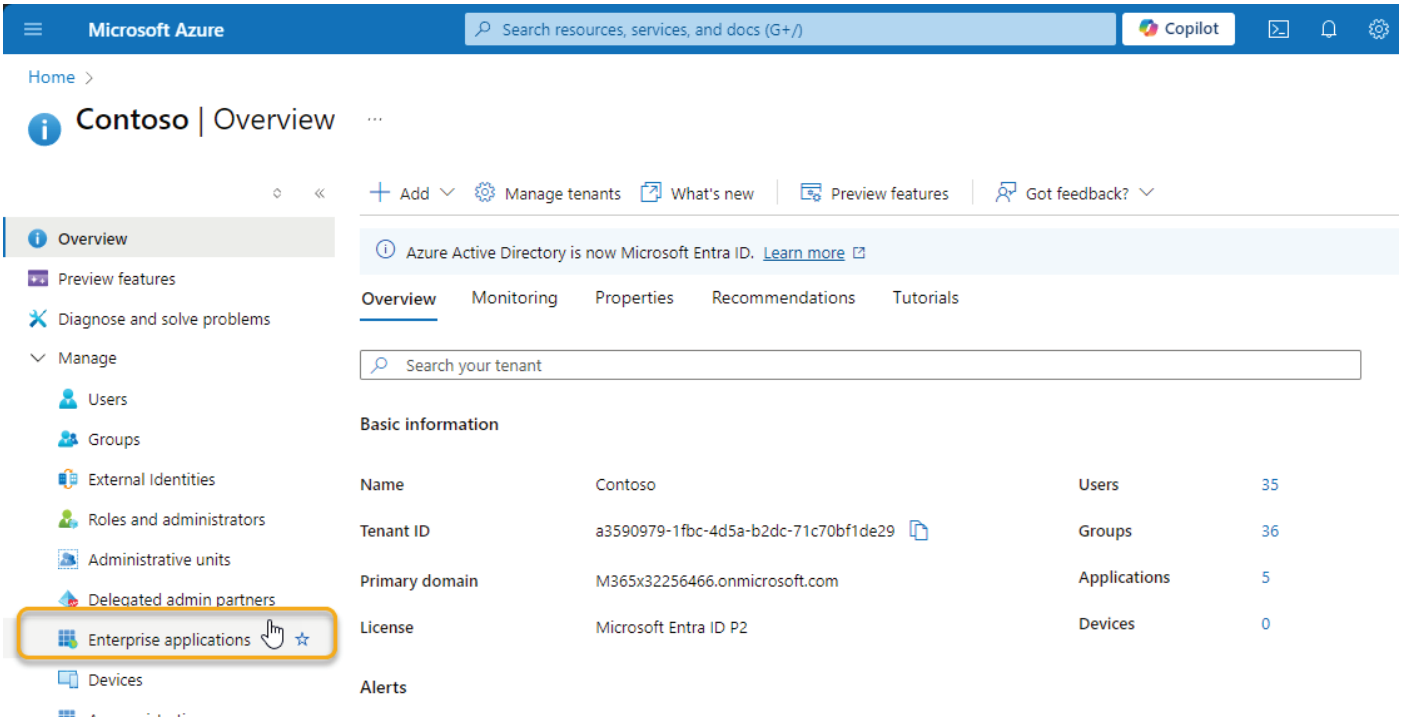
3 Approval is required, and the user can send an admin request



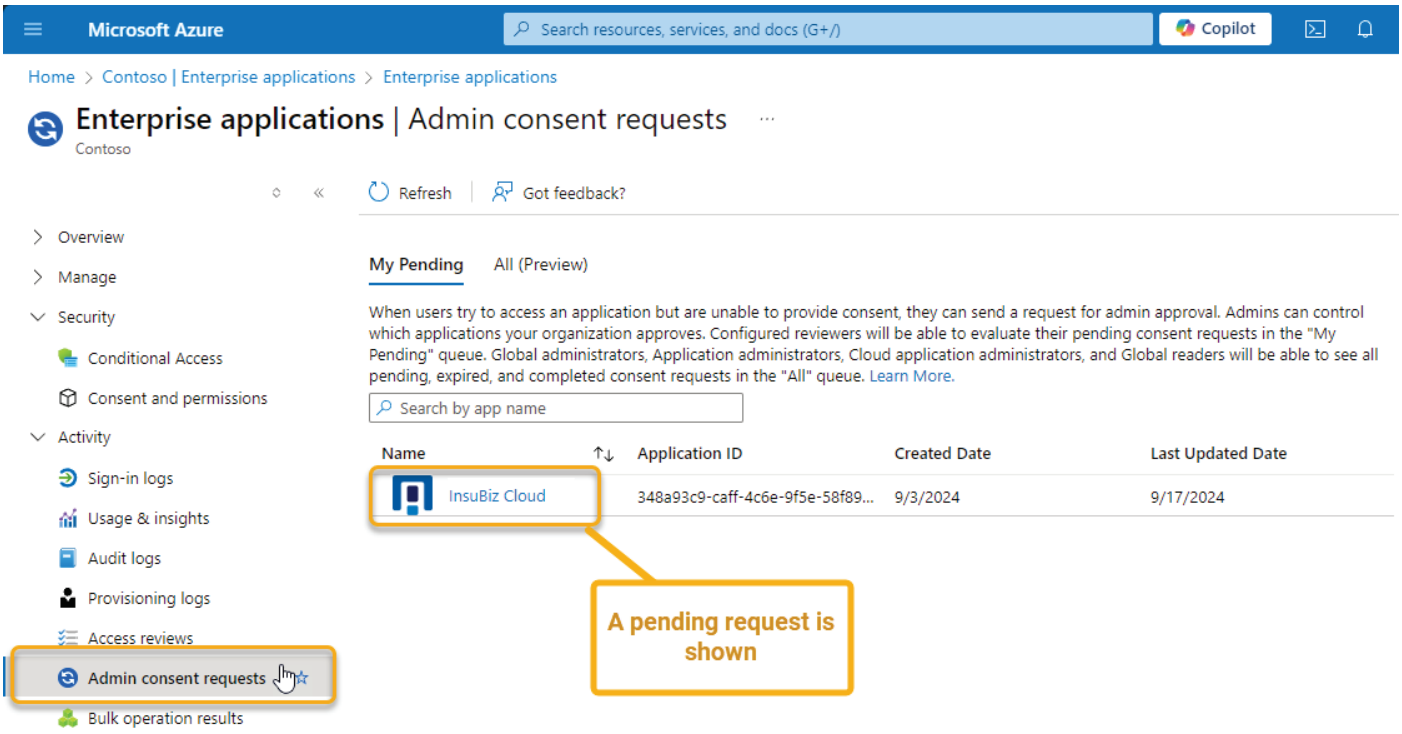
4 Sign in as Azure administrator on the organization



5 Go to Entra Id – Enterprise applications



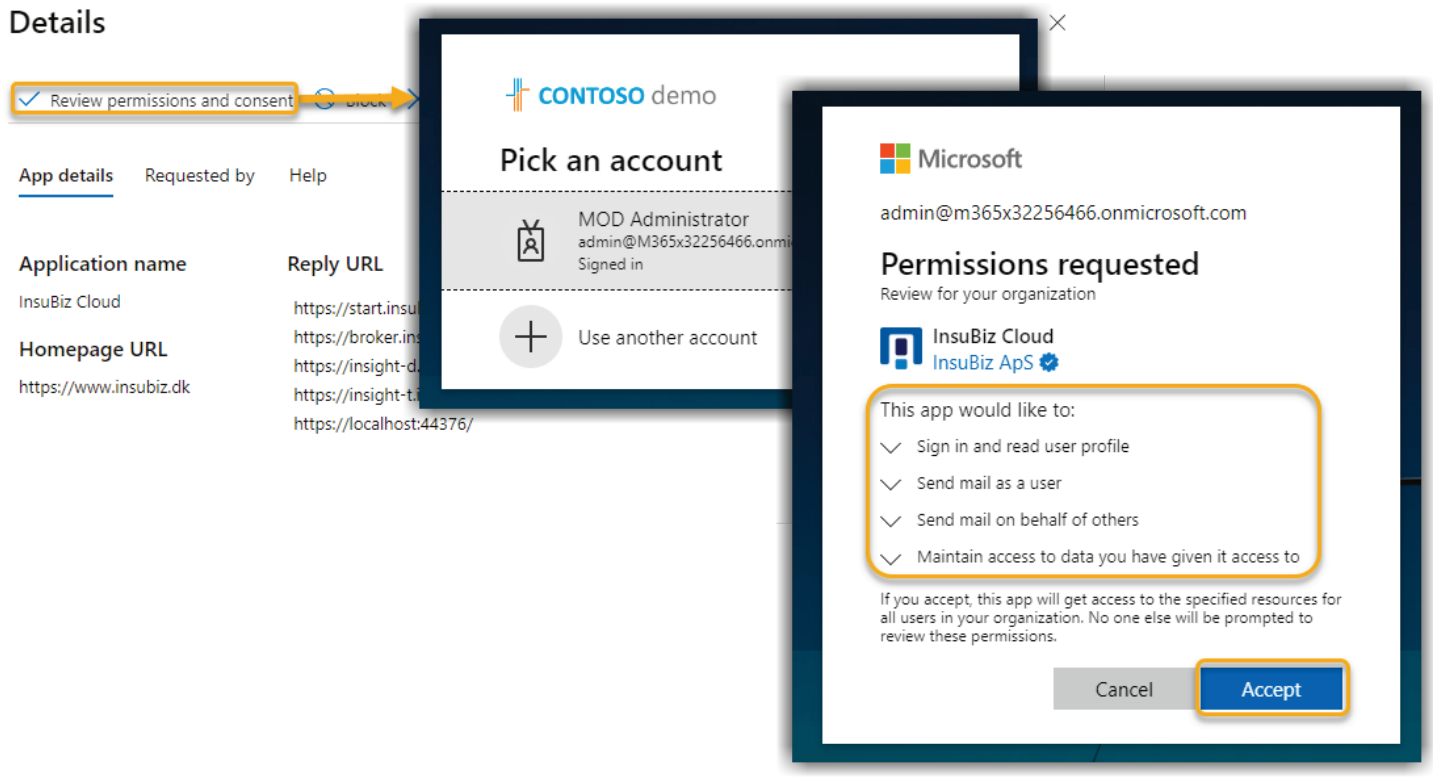
6 Go to Enterprise applications – Admin consent requests



Note: In some cases, the request may be shown with the name" InsuBiz InSight".

7 Click on the "InsuBiz Cloud" admin consent request

Open the request, revise the requested permissions and accept the request.



InsuBiz Cloud will now be added as an Enterprise Application in the organization with the required permissions.

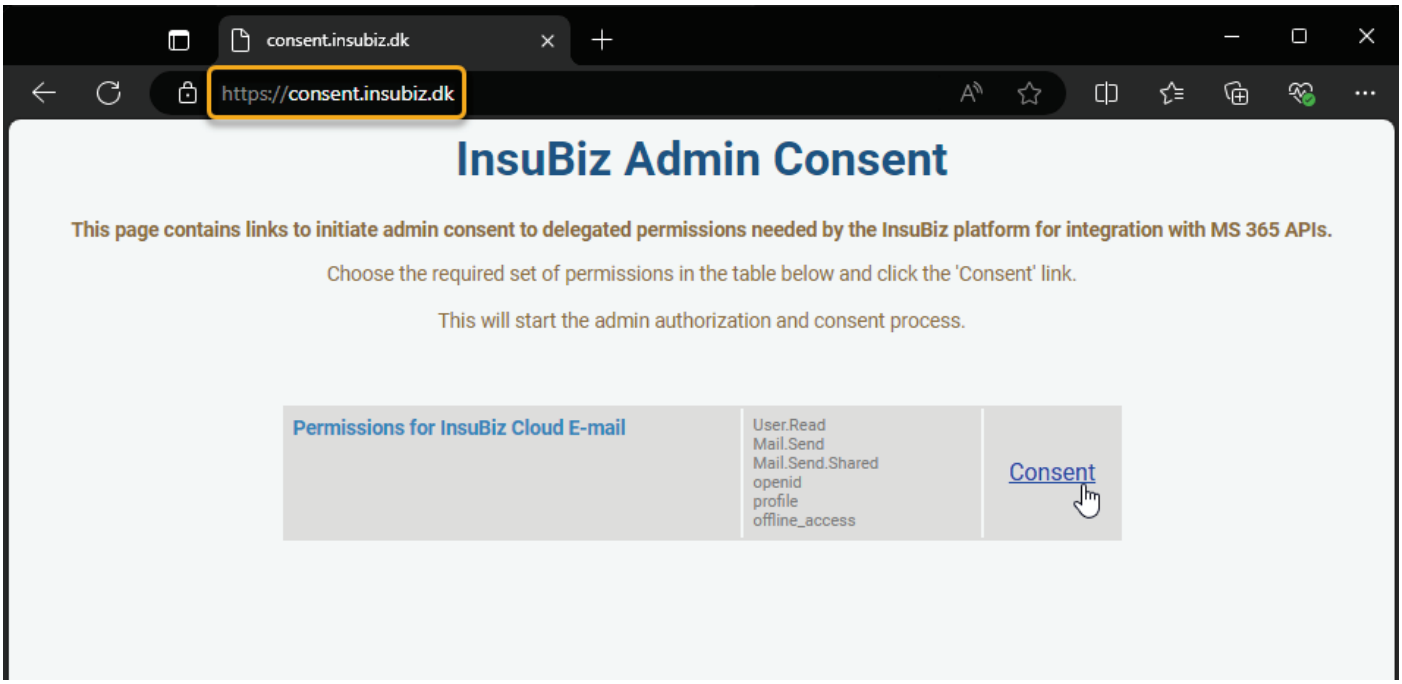
Admin consent using MS identity platform URL

It is possible to make an admin consent without a user request, by using the MS identity platform.

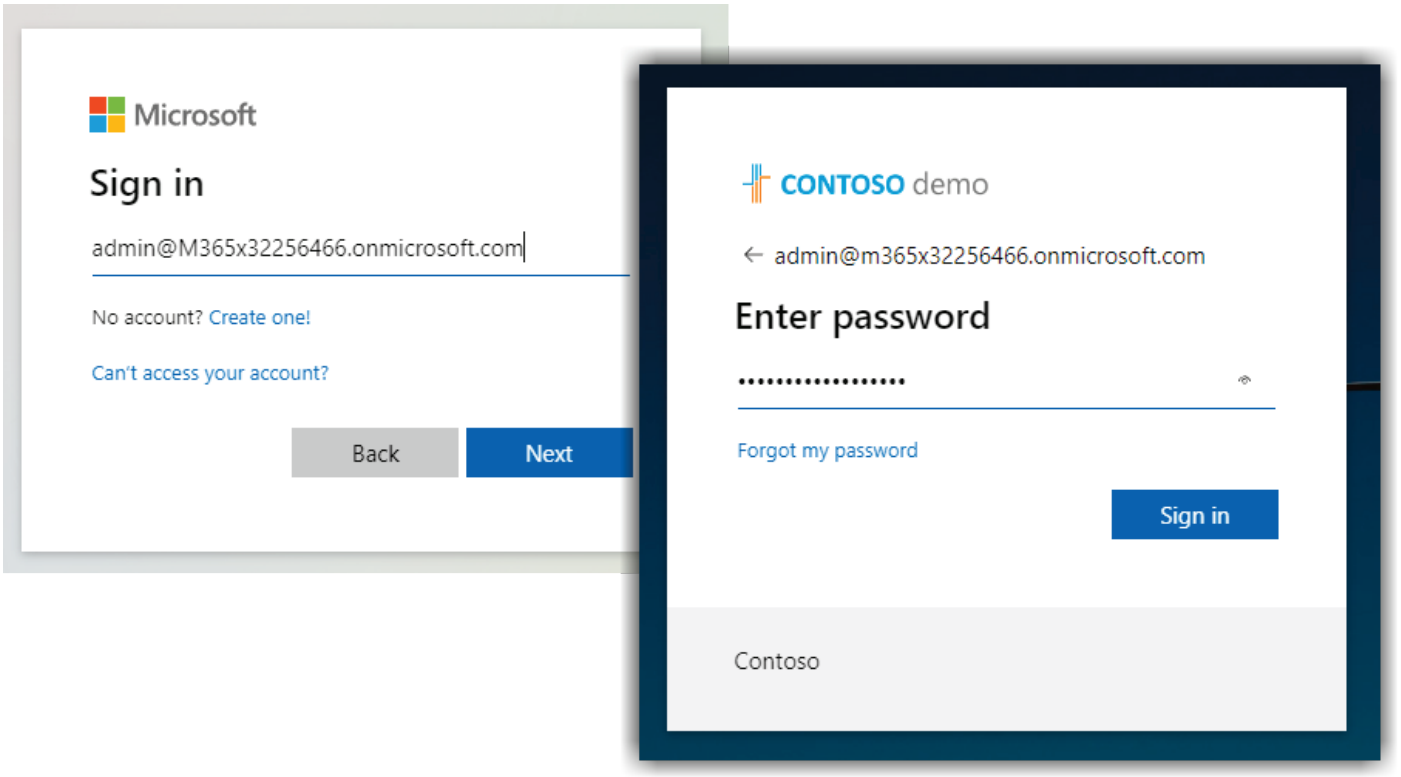
1 Go to the InsuBiz consent page to initiate the admin consent process

>> Start admin consent here <<

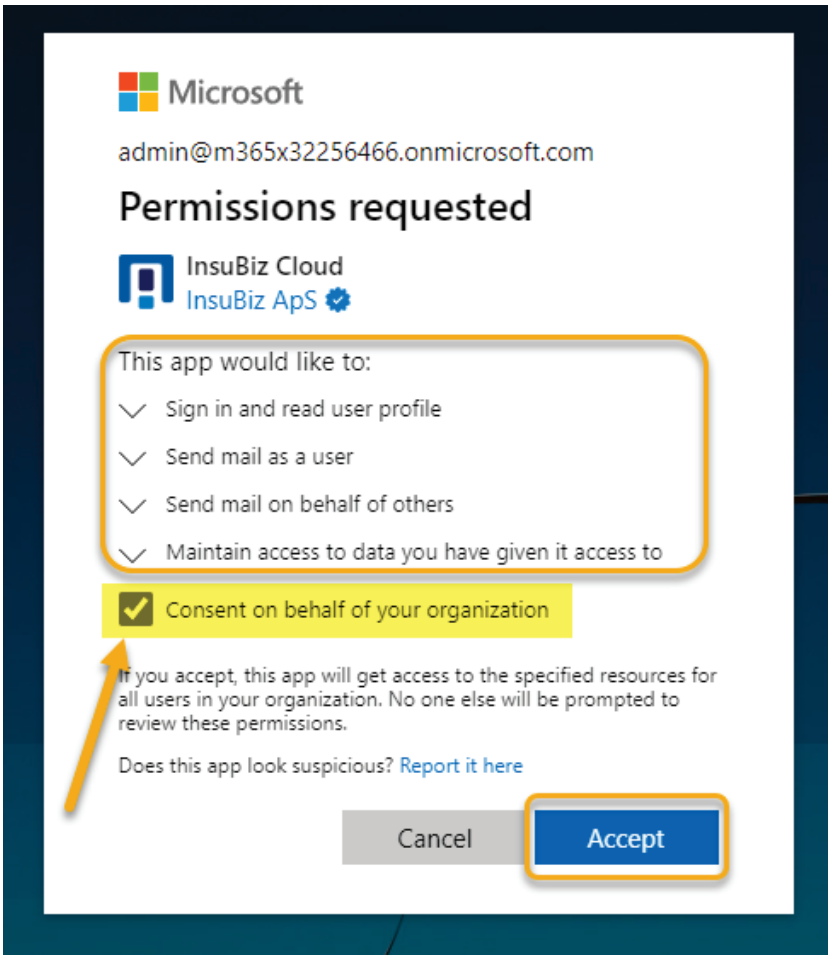
2 Click the "Consent' link for the required set of permissions



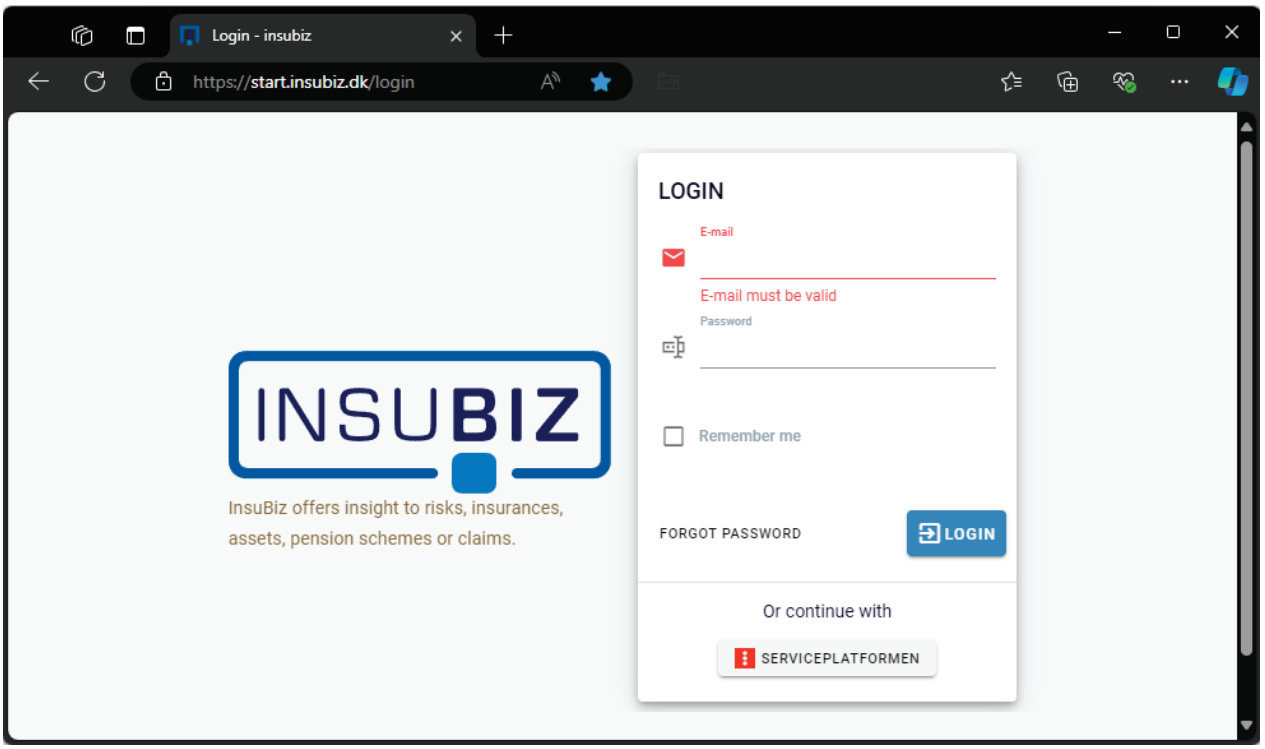
3 Sign in to an administrative account



4 Review requested permissions, make the consent on behalf of the organization and accept



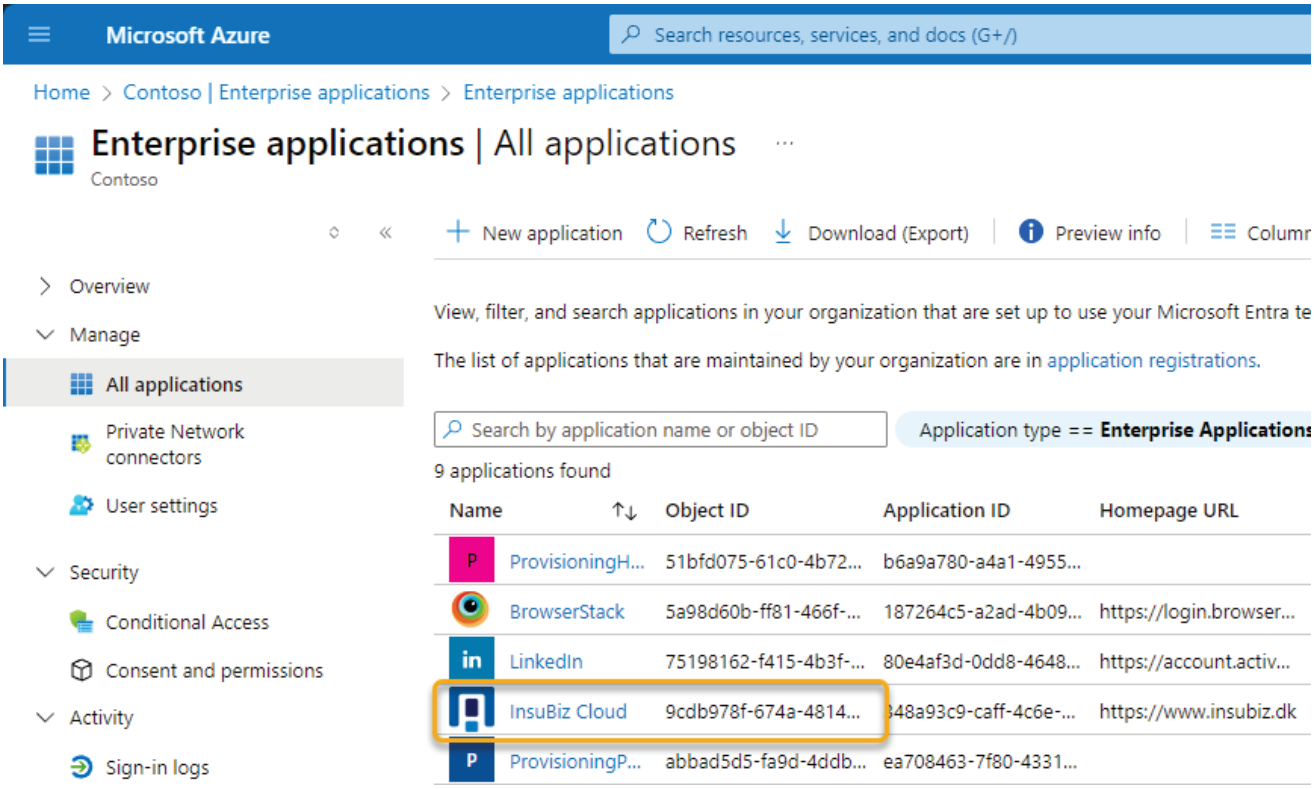
5 The consent has been registered, and you are directed to the InsuBiz Cloud login page



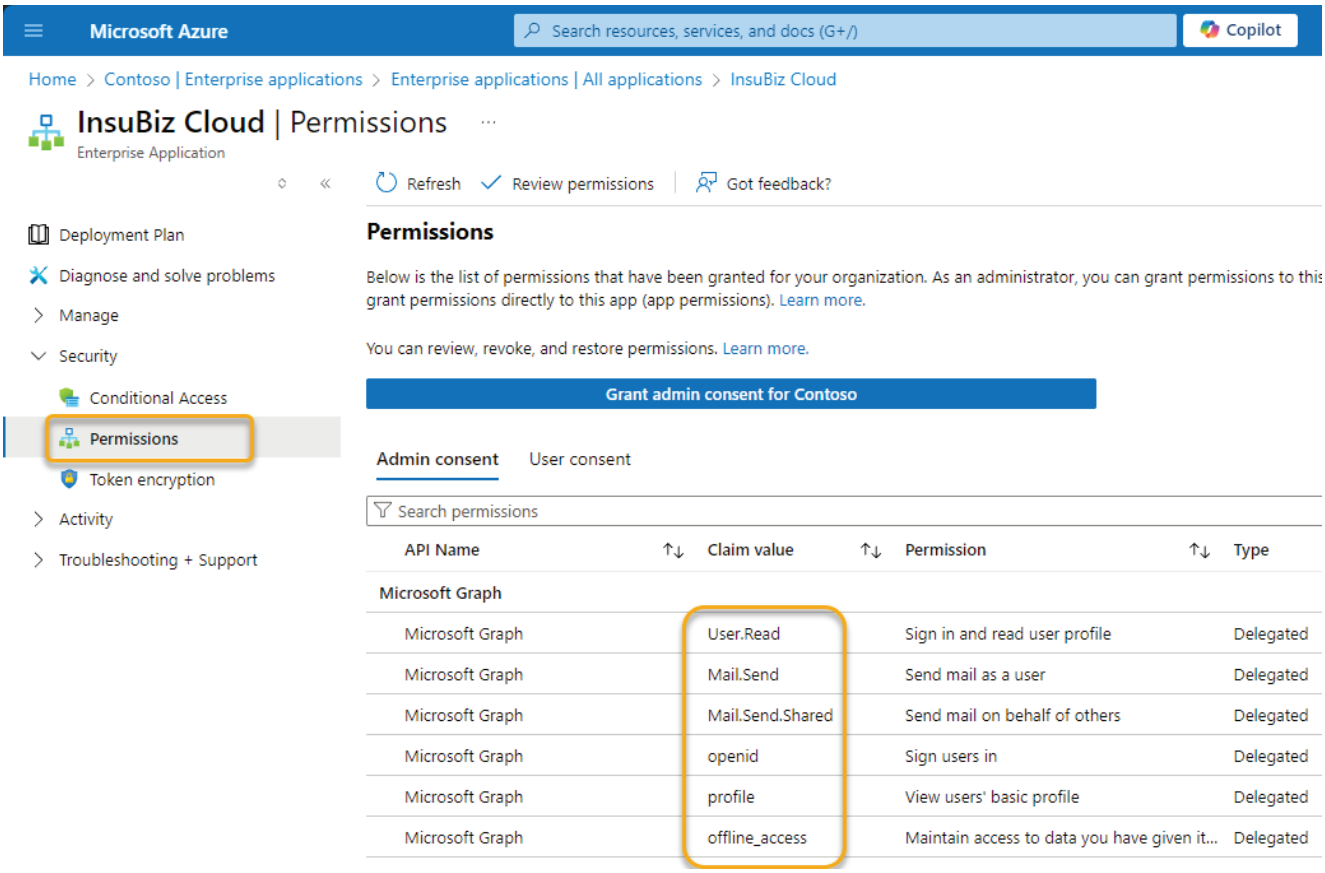
This page can just be closed, since the consent process has been completed.

Review the permissions in the Enterprise Application

1 Select the InsuBiz Cloud Enterprise Application

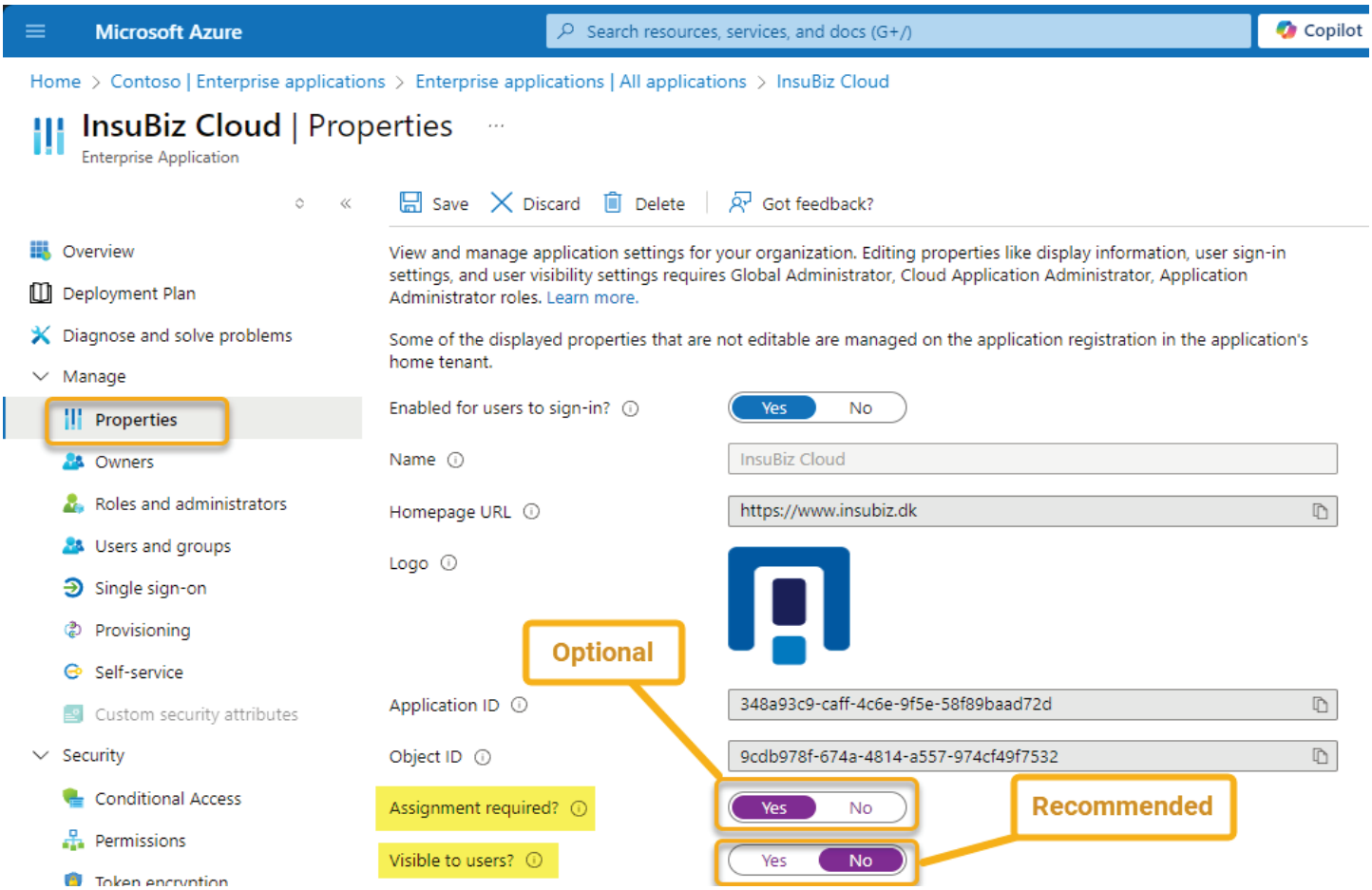


2 Review the consented permissions



Configuring the InsuBiz Cloud Application properties

1 Select the InsuBiz Cloud Enterprise Application and select the 'Properties' tab



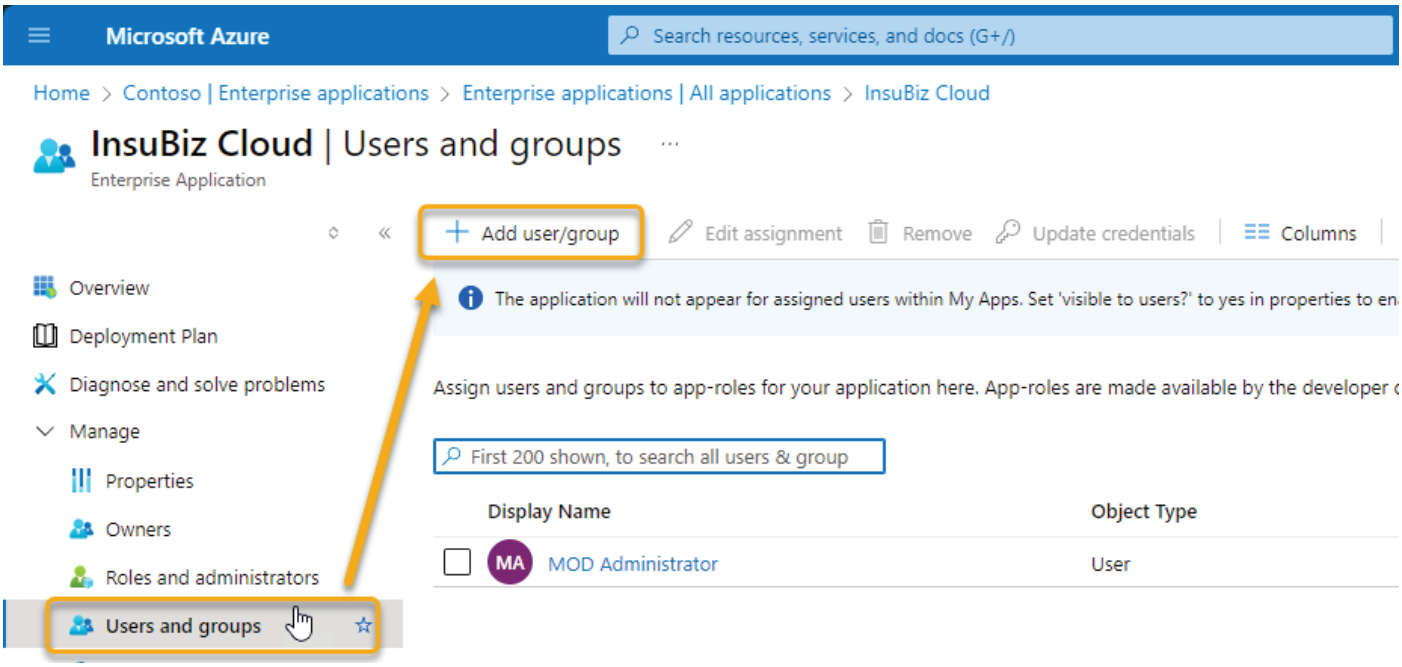
It is recommended to select 'No' for the property "Visible to users". By doing that, the application will not be visible in the user's app palette.

It is possible to narrow the access to the application further by selecting 'Yes' for the property "Assignment required". By doing this, specific users or groups must be assigned to the application to access it. (See next section)

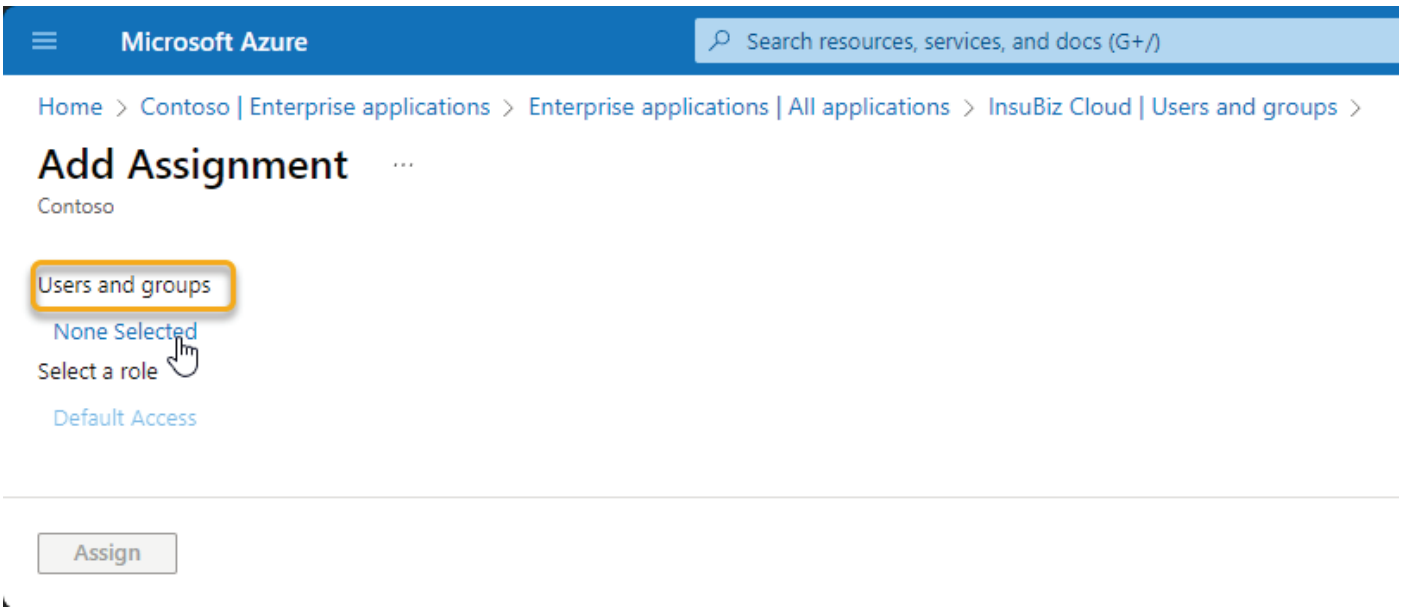
Configuring InsuBiz Cloud Application user assignment

If the “Assignment required” property is set to ‘Yes’, users must be assigned to the application either directly or via a group membership to access the integration functionality in InsuBiz Cloud.

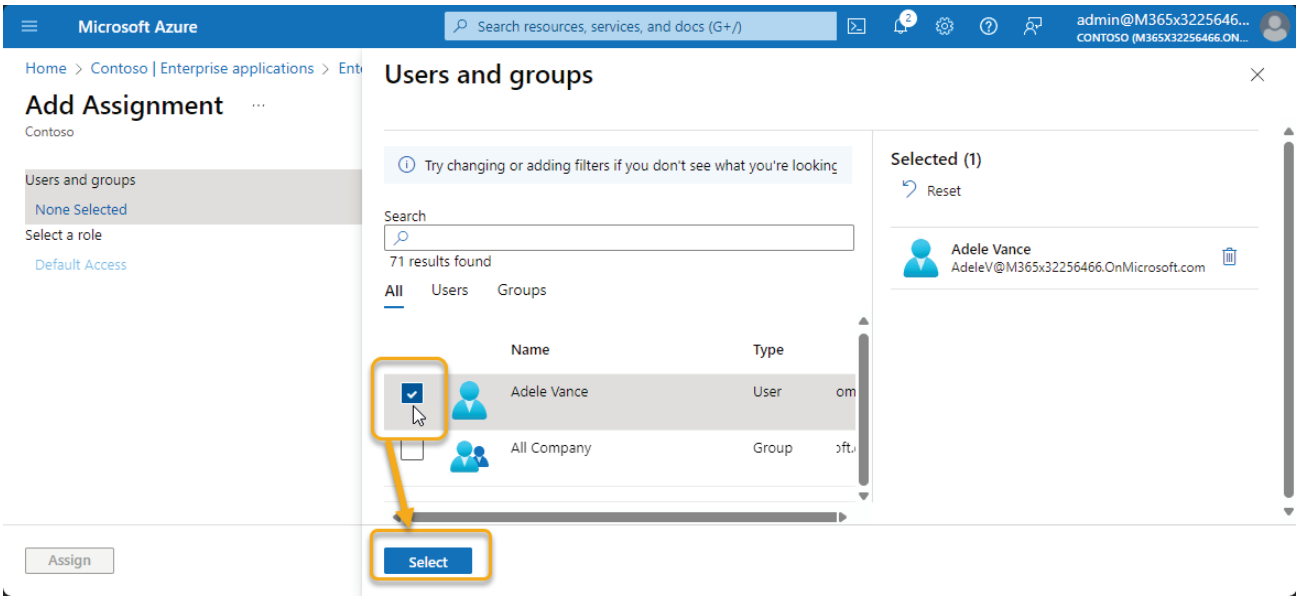
1 Select InsuBiz Cloud enterprise application, select the “Users and groups” tab and click +Add…



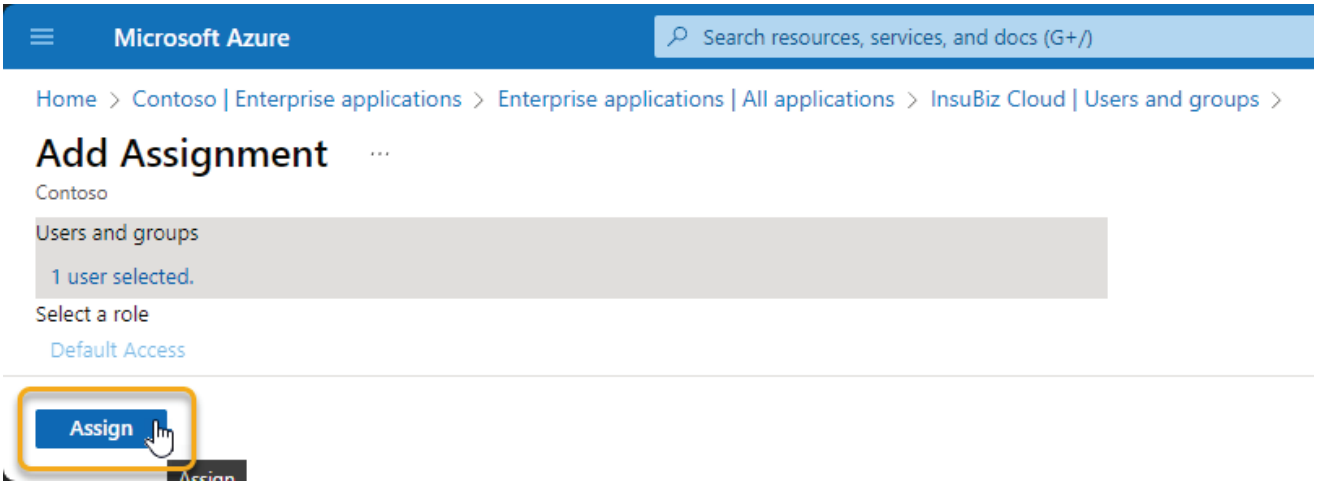
2 Click the link under “Users and groups”



3 Check all necessary users and groups and click “Select”



4 Click “Assign”



5 The users and group shas now been assigned to the Application